

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-289271

(43)Date of publication of application : 27.10.1998

(51)Int.Cl.

G06F 17/60

G06F 9/06

G06F 19/00

G06K 17/00

G07G 1/12

(21)Application number : 09-097241

(71)Applicant : HITACHI LTD

(22)Date of filing : 15.04.1997

(72)Inventor : HIROYA MASAOKI

ITO JUNJI

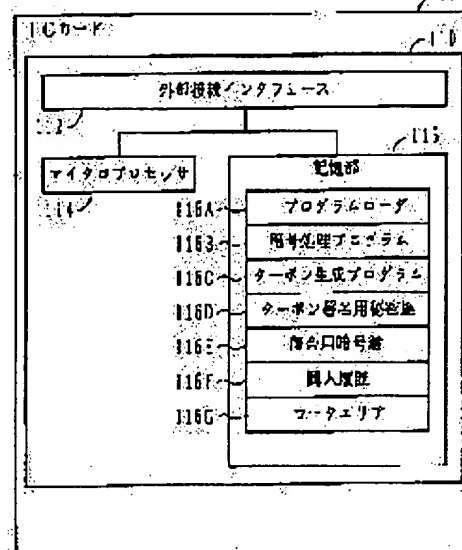
TERAMURA TAKESHI

(54) ELECTRONIC COUPON DEVICE AND INFORMATION PROCESSING SYSTEM USING IT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic coupon device and an information processing system which prevent a third person except a specific customer class from acquiring a generation program of a discount coupon and prevent the third person from using an invalid discount coupon.

SOLUTION: An IC card chip 110 of an IC card 100 that becomes an electronic coupon device has a storing part 116 which stores a program loader that loads an externally inputted program and a decoding key of cryptograph which decodes an enciphered discount coupon creation program, loads a discount coupon creation program which is externally inputted and generates a discount coupon through an external connection interface 112 by using the program loader, and also performs decoding processing of the loaded discount coupon creation program by using the decoding key of cryptograph.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-289271

(43)公開日 平成10年(1998)10月27日

(51)Int.Cl. ⁶	識別記号	F I
G 0 6 F 17/60		G 0 6 F 15/21 3 4 0 Z
9/06	5 5 0	9/06 5 5 0 A
19/00		G 0 6 K 17/00 L
G 0 6 K 17/00		G 0 7 G 1/12 3 2 1 P
G 0 7 G 1/12	3 2 1	G 0 6 F 15/30 3 5 0 A
審査請求 未請求 請求項の数8 O L (全 10 頁)		

(21)出願番号 特願平9-97241

(22)出願日 平成 9 年(1997) 4 月15日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72)発明者 広谷 政彰

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 伊藤 淳史

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 寺村 健

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

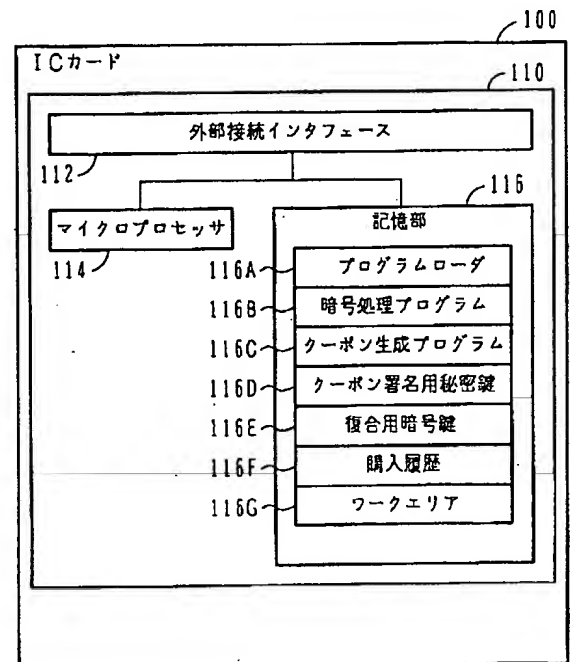
(74)代理人 弁理士 春日 巖

(54)【発明の名称】 電子クーポン装置及びそれを用いる情報処理システム

(57)【要約】 (修正有)

【課題】特定の顧客層以外の第三者による割引クーポンの生成プログラムの入手を防止し、第三者による不正な割引クーポンの使用を防止できる電子クーポン装置及び情報処理システム。

【解決手段】電子クーポン装置となるICカード100のICカードチップ110は、外部から入力されるプログラムをローディングするプログラムローダ及び暗号化された割引クーポン生成プログラムを復号化する復号用暗号鍵とを格納する記憶部116を有し、プログラムローダを用いて、外部接続インターフェース112を介して外部から入力される割引クーポンを生成するための割引クーポン生成プログラムをローディングするとともに、ローディングされた割引クーポン生成プログラムを復号用暗号鍵を用いて復号化する処理を行う。



1

【特許請求の範囲】

【請求項 1】外部に接続される機器とデータの入出力を行う外部接続インターフェースと、

この外部接続インターフェースを介して外部から入力されるプログラムをローディングするプログラムローダと、外部から入力される暗号化された割引クーポン生成プログラムを復号化する復号用暗号鍵とを格納する記憶部と、

この記憶部に格納された上記プログラムローダを用いて、上記外部接続インターフェースを介して外部から入力される割引クーポンを生成するための割引クーポン生成プログラムをローディングするとともに、ローディングされた割引クーポン生成プログラムを上記復号用暗号鍵を用いて復号化する処理を行うマイクロプロセッサとを備えたことを特徴とする電子クーポン装置。

【請求項 2】請求項 1 記載の電子クーポン装置において、

上記記憶部は、さらに、クーポン署名用秘密鍵を格納しており、

上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータに対して上記割引クーポン生成プログラムを用いて割引金額を求めるとともに、この割引金額を含む元のデータに対して、上記クーポン署名用秘密鍵を用いて電子的署名を施して割引クーポンを生成することを特徴とする電子クーポン装置。

【請求項 3】請求項 1 記載の電子クーポン装置において、

上記記憶部は、さらに、購入履歴を格納しており、

上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータ及び上記購入履歴に対して上記割引クーポン生成プログラムを用いて割引金額を求め、割引クーポンを生成することを特徴とする電子クーポン装置。

【請求項 4】請求項 1 記載の電子クーポン装置において、

上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータに対して上記割引クーポン生成プログラムを用いて割引金額を求め、さらに、購入者を識別するデータを付加して、割引クーポンを生成することを特徴とする電子クーポン装置。

【請求項 5】請求項 1 記載の電子クーポン装置において、

上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータに対して上記割引クーポン生成プログラムを用いて割引金額を求め、さらに、小売店を識別するデータを付加して、割引クーポンを生成することを特徴とする電子クーポン装置。

【請求項 6】請求項 1 記載の電子クーポン装置において、

2

上記外部接続インターフェースと上記プログラムローダと上記記憶部と上記マイクロプロセッサとは、接触式 IC カード若しくは非接触式 IC カード若しくは無線式 IC カードのいずれかに実装されていることを特徴とする電子クーポン装置。

【請求項 7】ネットワークを介して接続された購入者用情報処理装置と小売店用情報処理装置とメーカー用情報処理装置とから構成され、

上記購入者用情報処理は、上記メーカー用情報処理装置から上記ネットワークを介して送られてくる暗号化された割引クーポン生成プログラムを受信して、電子クーポン装置に書き込み、

上記小売店用情報処理装置は、上記電子クーポン装置の内部において復号化された上記割引クーポン生成プログラムが格納された電子クーポン装置に対して、購入内容のデータを出力し、上記電子クーポン装置から出力される秘密鍵によって電子的署名の施された割引クーポンに対して内部に予め格納されている公開鍵を用いてこの割引クーポンの有効性を検証することを特徴とする電子クーポン装置を用いる情報処理システム。

【請求項 8】請求項 7 記載の電子クーポン装置を用いる情報処理システムにおいて、

上記小売店用情報処理装置は、その内部に秘密鍵を有しており、この秘密鍵を用いて上記電子クーポン装置から発行された割引クーポンに対して電子的署名を施すとともに、

上記メーカー用情報処理装置は、上記小売店用情報処理装置から上記ネットワークを介して送られてくる上記割引クーポンに対して内部に予め格納されている公開鍵を用いてこの割引クーポンの有効性を検証することを特徴とする電子クーポン装置を用いる情報処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子クーポン装置及びそれを用いる情報処理システムに係り、特に割引クーポンに適用するに好適な電子クーポン装置及びそれを用いる情報処理システムに関する。

【0002】

【従来の技術】米国では、メーカーや小売店の販売促進を目的として、新聞広告などに商品を定価より安く購入できる割引クーポンを添付して配布している。商品の購入者は、その割引クーポンを小売店に持参して商品を購入すると商品を安く購入できる。

【0003】近年、これまで紙で作られていた割引クーポンを電子化する動きが盛んになってきている。米国では、割引クーポンを電子化してテレビ信号に乗せてテレビ広告と一緒に配布したり、電子化した割引クーポンを IC カード（スマートカードとも呼ばれる）に格納することが考えられている。テレビ信号を利用した割引クーポンについては、例えば、米国特許第 5 285 278 号

明細書や米国特許第5287181号明細書や米国特許第5523794号明細書等に記載されている。また、ICカードを利用した電子割引クーポンについては、例えば、米国特許第5380991号明細書に記載されている。

【0004】また、購入価格の割引方法には、単に特定商品の価格を所定の金額だけ安くするというだけではなく、一度に購入する商品の個数や商品の組合せ、もしくはそれまでの購入履歴などに応じて割引内容を変更する方法などがある。この方法に関連して、前述した米国特許第5380991号明細書には、購入履歴をICカードに記録しておき、その履歴に応じて割引率を変更することについても記載されている。購入履歴に基づく割引方法では、割引率や割引金額の計算は、基本的にICカードリーダーが接続されている端末装置か、この端末装置が接続されているホストコンピュータで行なっている。ICカードには、購入履歴など特定の購入者の割引内容を決断するために必要なデータと、どの商品が割引対象になっているかというデータが格納されており、端末装置あるいはホストコンピュータが割引金額を算出する際にそれらのデータを参照している。

【0005】

【発明が解決しようとする課題】近年、インターネットなどオープンなコンピュータネットワークが発達してきており、電子化したクーポンを配布するチャネルは、先に述べたテレビ広告も含め多様化する傾向にある。テレビ広告は、一般に不特定多数に対して情報を発信するが、コンピュータネットワークの電子メールなどを利用すると、特定の顧客層に対して情報を提供できるので、効率的なマーケティングが可能になる。具体的には、顧客別あるいは顧客層別に割引内容の異なるクーポンを発行することで、より効果的に購入意欲を刺激できるとともに、その割引クーポンがメーカー→顧客→小売店→顧客→メーカーと流通することで特定顧客の購買行動を収集できるようになる。

【0006】そこで、発明者らは、コンピュータネットワークの電子メールなどを利用して、電子化した割引クーポンを特定の顧客層に配布する方法について検討を行った。その検討の結果、割引内容を記した割引クーポン、あるいは購入内容に応じて割引クーポンを生成するプログラムをインターネットなどを通じて配布する方法を考えたが、かかるプログラムの配布方法では、特定の顧客層以外の第三者が不正にその割引クーポンの生成プログラムを入手して、不正に利用する恐れがあるという第1の問題があることが判明した。

【0007】また、割引クーポンがメーカーによって発行される場合、顧客へ割引金額相当の金銭は、小売店がメーカーから受け取ることになる。この場合、小売店が不正に入手した割引クーポンを用いて、不正な割引金額相当の金銭を搾取する恐れがあるという第2の問題があ

ることが判明した。

【0008】そこで、本発明の第1の目的は、特定の顧客層以外の第三者による割引クーポンの生成プログラムの入手を防止できる電子クーポン装置を提供することにある。

【0009】本発明の第2の目的は、第三者による不正な割引クーポンの使用を防止できる電子クーポン装置を用いる情報処理システムを提供することにある。

【0010】

【課題を解決するための手段】

(1) 上記第1の目的を達成するために、本発明は、外部に接続される機器とデータの入出力を行う外部接続インターフェースと、この外部接続インターフェースを介して外部から入力されるプログラムをローディングするプログラムローダと、外部から入力される暗号化された割引クーポン生成プログラムを復号化する復号用暗号鍵とを格納する記憶部と、この記憶部に格納された上記プログラムローダを用いて、上記外部接続インターフェースを介して外部から入力される割引クーポンを生成するための割引クーポン生成プログラムをローディングするとともに、ローディングされた割引クーポン生成プログラムを上記復号用暗号鍵を用いて復号化する処理を行うマイクロプロセッサとを備えるようにしたものである。かかる構成により、復号用暗号鍵を有しない第三者は、割引クーポン生成プログラムを入手できないため、特定の顧客層以外の第三者による割引クーポンの生成プログラムの入手を防止し得るものとなる。

【0011】(2) 上記(1)において、好ましくは、上記記憶部は、さらに、クーポン署名用秘密鍵を格納しており、上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータに対して上記割引クーポン生成プログラムを用いて割引金額を求めるとともに、この割引金額を含む元のデータに対して、上記クーポン署名用秘密鍵を用いて電子的署名を施して割引クーポンを生成するようにしたものである。かかる構成により、クーポン署名用秘密鍵を有しない第三者による割引クーポンの発行を防止し得るものとなる。

【0012】(3) 上記(1)において、好ましくは、上記記憶部は、さらに、購入履歴を格納しており、上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータ及び上記購入履歴に対して上記割引クーポン生成プログラムを用いて割引金額を求め、割引クーポンを生成するようにしたものである。かかる構成により、購入履歴に基づく割引方法を実現し得るものとなる。

【0013】(4) 上記(1)において、好ましくは、上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータに対して上記割引クーポン生成プログラムを用いて割引金額を求め、

5

さらに、購入者を識別するデータを付加して、割引クーポンを生成するようにしたものである。かかる構成により、購入者毎に効率的なマーケティングを行い得るものとなる。

【0014】(5)上記(1)において、好ましくは、上記マイクロプロセッサは、上記外部接続インターフェースを介して入力される購入内容のデータに対して上記割引クーポン生成プログラムを用いて割引金額を求め、さらに、小売店を識別するデータを付加して、割引クーポンを生成するようにしたものである。かかる構成により、小売店毎に効率的なマーケティングを行い得るものとなる。

【0015】(6)上記(1)において、好ましくは、上記外部接続インターフェースと上記プログラムロードと上記記憶部と上記マイクロプロセッサとは、接触式ICカード若しくは非接触式ICカード若しくは無線式ICカードのいずれかに実装するようにしたものである。

【0016】(7)上記目的を達成するために、本発明は、ネットワークを介して接続された購入者用情報処理装置と小売店用情報処理装置とメーカー用情報処理装置とから構成され、上記購入者用情報処理は、上記メーカー用情報処理装置から上記ネットワークを介して送られてくる暗号化された割引クーポン生成プログラムを受信して、電子クーポン装置に書き込み、上記小売店用情報処理装置は、上記電子クーポン装置の内部において復号化された上記割引クーポン生成プログラムが格納された電子クーポン装置に対して、購入内容のデータを出力し、上記電子クーポン装置から出力される秘密鍵によって電子的署名の施された割引クーポンに対して内部に予め格納されている公開鍵を用いてこの割引クーポンの有効性を検証するようにしたものである。かかる構成により、秘密鍵を有していない第三者による割引クーポンの不正使用を防止し得るものとなる。

【0017】(8)上記(7)において、好ましくは、上記小売店用情報処理装置は、その内部に秘密鍵を有しており、この秘密鍵を用いて上記電子クーポン装置から発行された割引クーポンに対して電子的署名を施すとともに、上記メーカー用情報処理装置は、上記小売店用情報処理装置から上記ネットワークを介して送られてくる上記割引クーポンに対して内部に予め格納されている公開鍵を用いてこの割引クーポンの有効性を検証するようにしたものである。かかる構成により、小売店による不正な割引金額相当の金銭の搾取を防止し得るものとなる。

【0018】

【発明の実施の形態】以下、図1～図6を用いて、本発明の一実施形態による電子クーポン装置及びそれを用いる情報処理システムについて説明する。最初に、図1を用いて、本発明の一実施形態による電子クーポン装置の構成について説明する。図1は、本発明の一実施形態に

6

よる電子クーポン装置の構成を示すブロック図である。

【0019】本実施形態による電子クーポン装置は、ICカード100によって構成されている。ICカード100上には、ICカードチップ110が実装されている。ICカードチップ110は、外部接続インターフェース112と、マイクロプロセッサ114と、記憶部116とから構成されている。外部接続インターフェース112は、ICカードチップ110と外部の情報処理装置とを接続する物理インタフェースである。マイクロプロセッサ114は、記憶部116に格納されているプログラムを実行する。記憶部116には、プログラムやデータが格納されている。

【0020】記憶部116は、プログラムロード格納エリア116Aと、暗号処理プログラム格納エリア116Bと、クーポン生成プログラム格納エリア116Cと、クーポン署名用秘密鍵格納エリア116Dと、復号用暗号鍵格納エリア116Eと、購入履歴格納エリア116Fと、ワークエリア116Gとを有している。プログラムロード格納エリア116Aには、インターネットを介して電子メールで送られてくる割引クーポン生成プログラムをローディングするためのプログラム(プログラムロードと呼ぶ)が、予め格納されている。プログラムロードとしては、例えば、サンマイクロシステムズがJavaカードAPIを提唱しており、それに関するドキュメントはサンマイクロシステムズのWWWサーバから入手できる。JavaカードAPIを用いることにより、ICカード100上で実行するプログラムを必要に応じてICカード100にローディングして実行することができる。従って、ICカード100上で実行する処理内容を容易に変更できるため、ICカード100を所有する顧客毎に、異なる割引を行うようにする場合にも、容易に割引内容の変更を行うことができる。

【0021】さらにICカード100は、必要な電子回路が1つのICカードチップ110に集積されており、かつ外部接続インターフェース112からの入出力をICカードチップ110のマイクロプロセッサ114で制御しているため、ICカードチップ110中に格納されているプログラムやデータを外部から自由に読み出せないようになっている。従って、電子化された割引クーポンのように偽造されては困るデータを生成・出力する割引クーポン生成プログラム等をICカード100上で実行させることは、セキュリティ上有効である。

【0022】暗号処理プログラム格納エリア116Bには、プログラムロード格納エリア116Aに格納されたプログラムロードを利用してローディングした暗号化されている割引クーポン生成プログラムを復号化するための暗号処理プログラムが、予め格納されている。

【0023】クーポン生成プログラム格納エリア116Cには、暗号処理プログラム格納エリア116Bに格納された暗号処理プログラムを用いて復号化された割引ク

7

ーボン生成プログラムが格納される。クーポン署名用秘密鍵格納エリア116Dには、クーポン生成プログラム格納エリア116Cに格納される割引クーポン生成プログラムによって作成される割引クーポンデータに電子的な署名を施すために使用する秘密鍵が、予め格納されている。なお、秘密鍵の詳細については、図3以降を用いて説明する。

【0024】復号用暗号鍵格納エリア116Eには、暗号処理プログラム格納エリア116Bに格納された暗号処理プログラムを用いて、電子メールで送られてきた割引クーポン生成プログラムを復号化するために使用する復号用暗号鍵が、予め格納されている。なお、復号用暗号鍵の詳細については、図3以降を用いて説明する。購入履歴格納エリア116Fには、購入者の過去の購入履歴が、商品の購入毎に格納される。なお、購入履歴は、割引クーポンにより割引の形態が、過去の購入履歴に応じて割引内容が変更されるものである場合に使用されるものである。従って、割引クーポンにより割引の形態が、商品の個数や組合せによって割引内容が変更されるものである場合には、購入履歴格納エリア116Fは備える必要がないものである。ワークエリア116Gは、プログラムを実行するために使用される。

【0025】ICカード100は、例えば、各商品を販売しているメーカーによって発行される。従って、記憶部116の中のプログラムロード格納エリア116Aと、暗号処理プログラム格納エリア116Bと、クーポン署名用秘密鍵格納エリア116Dと、復号用暗号鍵格納エリア116Eとに格納されるプログラムロードと、暗号処理プログラムと、クーポン署名用秘密鍵と、復号用暗号鍵は、ICカード100の発行時に予め格納されている。

【0026】次に、図2を用いて、本発明の一実施形態による電子クーポン装置を用いて割引サービスを行う場合に使用するシステムの構成について説明する。図2は、本発明の一実施形態による電子クーポン装置を用いる情報処理システムのブロック図である。

【0027】メーカー用情報処理装置210と、購入者用情報処理装置220と、小売店用情報処理装置（POS端末）230とは、コンピュータネットワーク200によって互いに接続されている。コンピュータネットワーク200は、インターネットのようなオープンなネットワークでもよいし、専用ネットワークでもよいものである。また、メーカー用情報処理装置210と購入者用情報処理装置220が接続されているコンピュータネットワークと、メーカー用情報処理装置210と小売店用情報処理装置230が接続されているコンピュータネットワークが、それぞれ、独立に接続されているものであってもよいものである。

【0028】購入者用情報処理装置220は、ICカード100に対して情報を読み出す／書き込むためのIC

8

カードリーダライタ222に接続されている。

【0029】メーカーが、メーカー用情報処理装置210からコンピュータネットワーク200を介して特定の顧客に対して送った割引クーポン生成プログラムを含む電子メールは、購入者用情報処理装置220によって配達される。ここで、電子メールで送られる割引クーポン生成プログラムは、メーカー用情報処理装置210が所有する暗号鍵を用いて暗号化されている。暗号鍵としては、例えば、暗号鍵Kを用いる。

【0030】電子メールを受け取った購入者は、購入者用情報処理装置220によって受信した割引クーポン生成プログラムを、ICカードリーダライタ222を用いて、自分が所有するICカード100の中のICカードチップ110に格納する。このプログラムの格納処理については、図4を用いて、後述する。格納された割引クーポン生成プログラムは、ICカードチップ110に予め格納されている復号鍵を用いて復号化される。ここで、復号鍵としては、例えば、暗号鍵Kに対して対称性を有する復号鍵Kを用いる。従って、コンピュータネットワーク200を介して特定の顧客に対して送られた割引クーポン生成プログラムは、復号鍵Kを有していない第三者には、復号解読が不可能であるため、第三者による不正を防止することができる。なお、暗号鍵及び復号鍵としては、上述したように、対称な鍵の他に、後述する公開鍵と秘密鍵のように非対称性を有するものを用いることもできる。

【0031】小売店用情報処理装置230は、ICカードリーダライタ232及び商品のバーコードを読み取るためのバーコードスキャナ234に接続されている。商品の購入者は、小売店において、割引クーポン生成プログラムの格納されているICカード100Aを提示して商品を購入する。購入された商品の品名は、バーコードスキャナ234によって、小売店用情報処理装置230に読み込まれる。小売店用情報処理装置230は、購入された商品の品名の他に、その商品の単価や購入個数等のデータを、ICカードリーダライタ232を用いて、購入者が提示したICカード100Aに書き込む。書き込まれたデータは、ICカードチップ110Aに入力する。ICカードチップ110Aに格納されている割引クーポン生成プログラムは、入力された商品の品名、その商品の単価や購入個数等のデータに基づいて、割引金額を計算する。計算された割引金額等のデータは、ICカードリーダライタ232を介して、小売店用情報処理装置230に入力される。小売店用情報処理装置230の表示部に表示された合計金額や、割引金額等に基づいて、購入者が商品を購入することによって、購入者は、割引クーポンを使用して割引購入を行うことができる。

【0032】また、ICカードチップ110Aは、ICカードリーダライタ232を介して、小売店用情報処理装置230に出力するデータの最後に、割引金額等のデ

9

ータに対して秘密鍵を用いて作成した電子的な署名データを付加している。秘密鍵を用いて電子的な署名データの詳細については、後述するが、これは、第三者及び小売店による不正を防止するために用いられる。

【0033】ここで、秘密鍵としては、例えば、小売店用情報処理装置230が予め保持している公開鍵Pに対して非対称性を有する秘密鍵Sを用いる。秘密鍵Sと公開鍵Pを生成する方法としては、例えば、RSA暗号がある。従って、例えば、不正な第三者が、コンピュータネットワーク200を介して送られた暗号化された割引クーポン生成プログラムを不正に入手して解読し、ICカードにロードしたとしても、このICカードの中には、秘密鍵Sは格納されていない。そこで、このICカードを用いて商品を購入しようとしても、電子的な署名データが付加されていないため、小売店用情報処理装置230は、正規の割引による購入としては受け付けられないため、第三者による不正な購入を防止することができる。また、電子的な署名データのようなデータが付加されている場合には、小売店用情報処理装置230が予め保持している公開鍵Pを用いて、署名データを復号化して、割引金額等のデータとの一致を確認することにより、不一致の場合は、正規の割引による購入としては受け付けられないため、第三者による不正な購入を防止することができる。

【0034】また、小売店用情報処理装置230に入力された割引金額等のデータに対して電子的な署名データが付加されたデータは、コンピュータネットワーク200を介して、メーカー用情報処理装置210に送られる。メーカー用情報処理装置210は、公開鍵Pを有しており、送られてきた電子的な署名データに対して公開鍵Pを用いて、元の割引金額等のデータを復号する。この復号されたデータと、送られてきた割引金額等のデータとの一致を確認する。もし、小売店が、割引金額等のデータを改ざんして、不正な割引金額等のデータを作成したとしても、小売店用情報処理装置230は、秘密鍵Sは有していないため、正しい電子的な署名データを付加することはできないため、正規の割引としては受け付けられないため、小売店による不正な割引請求を防止することができる。

【0035】次に、図3～図6を用いて、各情報処理装置における処理内容について説明する。最初に、図3を用いて、メーカー用情報処理装置210における処理内容について説明する。図3は、本発明の一実施形態による電子クーポン装置を用いる情報処理システムの中のメーカー用情報処理装置における処理内容を示すフローチャートである。

【0036】ステップ310において、メーカー用情報処理装置210は、割引クーポン生成プログラムを暗号鍵Kを用いて暗号化する。ここで、割引クーポン生成プログラムは、メーカー用情報処理装置210に格納

10

されている。割引クーポン生成プログラムは、JAVA言語に代表されるインタプリタ言語で記述されている。ICカードのネイティブコードであってもよいものである。割引クーポン生成プログラムの処理内容は、小売店用情報処理装置230からICカードリーダライタ232を経由して入力された購入データに基づいて割引金額を算出し、割引金額を含むデータに対して電子的に署名を行ない、署名付きデータ（割引クーポンと称する）をICカードリーダライタ232を経由して小売店用情報処理装置230に出力するものである。

【0037】割引クーポン生成プログラムによる割引金額算出処理の一例について、以下に説明する。割引クーポン生成プログラムにおける割引内容が、商品Aの購入個数が10個未満ならば1個につき50円引き、商品Aの購入個数が10個以上100個未満ならば1個につき80円引き、商品Aの購入個数が100個以上ならば1個につき100円引きにするというものである場合、購入内容が「A商品を20個購入」ならば、割引金額は $80 \times 20 = 1600$ 円となる。別の例として、複数の商品を組み合わせて割引金額を算出する処理や、過去の購入履歴をICカードチップ110の購入履歴エリア16に記憶させておいて、今回の購入内容と過去の購入履歴を組み合わせて割引金額を算出するものなどがある。

【0038】また、暗号鍵Kとしては、購入者の所持するICカード100の中のICカードチップ110に予め格納されている復号用暗号鍵Kと対称性を有するものとする。なお、暗号鍵及び復号鍵としては、上述したように、対称な鍵の他に、公開鍵と秘密鍵のように非対称性を有するものを用いることもできる。

【0039】ステップ320において、メーカー用情報処理装置210は、暗号化されたデータを、コンピュータネットワーク200を介して、電子メールなどで特定の顧客に送る。顧客は、所有するICカードの中に予め格納されている復号鍵Kを用いて送られてきた割引クーポン生成プログラムを復号化することができる。

【0040】従って、復号鍵Kを有しない第三者は、暗号化されたデータを不正に受信しても、復号化できず、割引クーポン生成プログラムの第三者による不正使用を防止できる。

【0041】なお、メーカーが、顧客を複数のグループG1、G2、G3に分類して、それぞれのグループに対して異なる割引内容の割引クーポン生成プログラムを送りたい場合には、複数のグループG1、G2、G3が所有するそれぞれのICカードに対して、異なる復号鍵K1、K2、K3を予め格納しておく。そして、それぞれの復号鍵K1、K2、K3に対応した暗号鍵K1、K2、K3を用いて、異なる割引内容の割引クーポン生成プログラムを暗号化することにより、それぞれのグループに対して異なる割引内容の割引クーポン生成プロ

11

ラムを送ることが可能である。

【0042】次に、図4を用いて、購入者用情報処理装置220及び購入者の所有するICカード100における処理内容について説明する。図4は、本発明の一実施形態による電子クーポン装置を用いる情報処理システムの中の購入者用情報処理装置及び購入者の所有するICカードにおける処理内容を示すフローチャートである。

【0043】ステップ410において、購入者用情報処理装置220は、電子メールを受信する。次に、ステップ420において、購入者用情報処理装置220は、ICカードリーダライタ222を経由して、ICカード100の中のICカードチップ110に受信メールに含まれる暗号化されたデータ列を入力する。入力されたデータ列は、ICカードチップ110中の記憶部116のワークエリア116Gに格納される。ここで、もし、ICカード100が、まだICカードリーダライタ222に挿入されていないならば、ICカード100をICカードリーダライタ222に挿入する。

【0044】ステップ430において、ICカードチップ110中のマイクロプロセッサ114は、記憶部116のプログラムロード格納部116Aに予め格納されているプログラムロードの処理に基づいて、暗号処理プログラム格納エリア116Bに予め格納されている暗号処理プログラム及び復号用暗号鍵格納エリア116Eに格納されている復号用暗号鍵を用いて、ワークエリア116Gに格納されているデータ列を復号して、クーポン生成プログラムを生成する。

【0045】ステップ440において、マイクロプロセッサ114は、生成された割引クーポン生成プログラムをクーポン生成プログラム格納エリア116Cに格納する。

【0046】購入者は、商品を購入するときに、割引クーポン生成プログラムが格納されているICカード100を小売店に持参する。

【0047】次に、図5を用いて、小売店用情報処理装置230及び購入者が小売店に所持したICカード100Aにおける処理内容について説明する。図5は、本発明の一実施形態による電子クーポン装置を用いる情報処理システムの中の小売店用情報処理装置及び購入者が所持したICカードにおける処理内容を示すフローチャートである。

【0048】購入者は、ICカード100Aを持参して小売店に行き、購入したい商品及びICカード100Aを小売店に提示して、商品を購入する。その際、以下に示すような処理が行われる。

【0049】ステップ510において、小売店用情報処理装置230は、バーコードスキャナ234によって読み取られた購入商品のバーコードを入力する。次に、ステップ520において、小売店用情報処理装置230は、購入者が持参したICカード100AがICカード

12

リーダライタ232に挿入されたか否かを判断する。

【0050】ICカード100AがICカードリーダライタ232に挿入されると、ステップ530において、小売店用情報処理装置230は、ICカードリーダライタ232を経由して、ICカード100AのICカードチップ110Aに購入内容を入力する。購入内容としては、品名を示すバーコードデータ及び購入個数等である。なお、ここで、小売店を識別するためのデータも一緒に入力してもよい。小売店の識別データとしては、小売店毎に予め定められている小売店IDや、小売店用情報処理装置230毎に予め与えられているPOSIDを用いることができる。小売店が複数の小売店用情報処理装置230を所有している場合には、小売店IDを用いるようにするが、小売店が1台の小売店用情報処理装置230を所有している場合には、POSIDによって小売店を識別することができるため、POSIDを用いることができる。

【0051】次に、ステップ540において、ICカードチップ110A中のマイクロプロセッサ114は、記憶部116の割引クーポン生成プログラム格納エリア116Cに格納されている割引クーポン生成プログラムを用いて、購入内容（購入品名、購入個数）に基づいて割引金額を計算する。計算された割引金額は、ワークエリア116Gに格納される。割引内容が、購入履歴に応じて割引金額が求められるものである場合には、購入履歴格納エリア116Fに格納されている購入履歴のデータを用いて、割引金額が計算される。

【0052】次に、ステップ550において、マイクロプロセッサ114は、割引クーポン生成プログラム及びクーポン署名用秘密鍵格納エリア116Dに格納されているクーポン署名用秘密鍵Sを用いて、割引金額と購入内容を含むデータに電子的署名を施した割引クーポンを生成する。

【0053】ここで、図6を用いて、ステップ550において生成された割引クーポンのデータ構成について説明する。図6は、本発明の一実施形態による電子クーポン装置によって生成される割引クーポンのデータ構成の説明図である。

【0054】図6(A)に示すように、割引クーポンは、元となるデータと、このデータに対して付与された電子的署名からなっている。電子的署名の付与は、次のようにして行われる。即ち、元となるデータにHash（ハッシュ）関数を掛けて、元データよりバイト数の小さいデータとする。このデータを、クーポン署名用秘密鍵Sを用いて暗号化して、電子的署名とする。

【0055】また、元となるデータは、図6(B)に示すような構成となっている。即ち、元となるデータは、小売店を識別する小売店IDと、小売店における発行の順番を示すSer. Noと、購入者を識別するためのICカード100Aの所有者を示すUserIDと、ステ

13

ップ540において求められた割引金額と、ステップ530において入力した購入内容から構成されている。

【0056】ステップ560において、マイクロプロセッサ114は、外部接続インタフェース112を介して割引クーポンを出力し、ICカードリーダー232を経由して、小売店用情報処理装置230に割引クーポンを出力する。

【0057】次に、ステップ570において、小売店用情報処理装置230は、予め格納してある公開鍵Pを利用して、割引クーポンの有効性を検証する。公開鍵Pは、割引クーポンに電子的に署名する際に使用した秘密鍵Sと対をなす暗号鍵であり、メーカーから小売店に事前に配布されている。割引クーポンの中にある電子的署名を、公開鍵Pを用いて復号化する。この復号化されたデータと、割引クーポンの中の元となる購入内容等のデータにHash（ハッシュ）関数を掛けて求めたデータとが一致しているとき、割引クーポンが有効であると判断する。

【0058】従って、クーポン生成用秘密鍵Sを有していない不正な第三者が割引クーポンを発行したとしても、正しい電子的署名が付与されていないため、その割引クーポンは、無効なものとされる。

【0059】ここで、割引クーポンが有効ならば、小売店の店員は、その割引クーポンに含まれている割引金額に相当する金銭を購入金額の合計から減算して、商品を販売する。

【0060】小売店情報処理装置230に格納された割引クーポンは、すぐにメーカー用情報処理装置210に送付してもよいし、一日ごと一ヶ月毎などのように、定期的にまとめて送付してもよいものである。

【0061】割引クーポンが送られたメーカーは、秘密鍵Sと対になるメーカーが所有する公開鍵Pを利用して割引クーポンの有効性を検証する。有効性が検証できた場合には、メーカーは、小売店に割引クーポンに含まれる割引金額相当の金銭を渡す。

【0062】小売店が所有しているのは、公開鍵Pのみであり、秘密鍵Sは、有していない。従って、小売店が、不正な割引クーポンを発行して、不正な割引金額相当の金銭を受け取ろうとしても、そのような割引クーポンは無効となるため、小売店による不正を防止することができる。

【0063】また、割引クーポンに購入者や小売店を識別するデータが含まれているため、メーカーは、それを取り出して購入内容とともにデータベースなどに格納すれば、有用なマーケティングデータにできる。

【0064】なお、以上の説明では、接触式ICカードについて説明したが、外部接続インタフェース112に電磁波などの媒体の送受信装置を利用し、ICカードリーダー222、232に同様の外部インタフェースを有するものを利用すれば、非接触式あるいは無線式I

14

Cカードを用いることもできる。

【0065】また、電子的署名は、購入者が所有するICカード内の秘密鍵によって購入者の署名だけを施すようにしているが、さらに、小売店用情報処理装置内に秘密鍵を保持させ、小売店からメーカーに割引クーポンを送る場合に、小売店の電子的署名を施すようにしてもよい。この小売店の電子的署名は、図6（A）に示したデータと購入者の電子的署名からなる全データに対して、ハッシュ関数を掛けて求めた所定のバイト数のデータを、小売店の秘密鍵によって暗号化する。また、小売店の有する秘密鍵は、各小売店毎に異なるようにすることもできる。小売店毎に異なる秘密鍵を用いることにより、どこの小売店の小売店用情報処理装置によって署名がなされたかが判明するため、小売店の不正を防止することができる。

【0066】以上説明したように、本実施形態によれば、暗号鍵を用いて割引クーポン生成プログラムを暗号化した上で配布するため、安全に割引クーポン生成プログラムを配布することができる。

【0067】また、コンピュータネットワークを介して割引クーポン生成プログラムを配布できるため、商品のメーカーは特定の顧客ごとに割引内容が異なる割引クーポンの発行を容易に行えるものとなる。

【0068】また、割引クーポンの発行時には、購入金額等のデータに対して、秘密鍵を用いて電子的署名を施すようにしており、また、割引クーポンを生成するための秘密鍵は、ICカード中に隠蔽されているので、購入者や小売店などによる偽造を防ぐことができる。

【0069】さらに、小売店用情報処理装置は、割引処理を行なうに際して、基本的に割引クーポンの電子的署名の有効性のみを検証すればよいので、割引方法が変更されても、小売店用情報処理装置の内部のプログラムの改造等を必要としないものである。

【0070】さらに、割引クーポンの中に購入者を識別するデータと商品を販売した小売店を識別するデータが入っているため、メーカーは、購入者の購買行動を収集することができるので、効率的にマーケティングすることが可能になる。

【0071】

【発明の効果】本発明によれば、電子クーポン装置における特定の顧客層以外の第三者による割引クーポンの生成プログラムの入手を防止できる。

【0072】また、本発明によれば、電子クーポン装置を用いる情報処理システムにおける第三者による不正な割引クーポンの使用を防止できる。

【図面の簡単な説明】

【図1】本発明の一実施形態による電子クーポン装置の構成を示すブロック図である。

【図2】本発明の一実施形態による電子クーポン装置を用いる情報処理システムのブロック図である。

15

【図3】本発明の一実施形態による電子クーポン装置を用いる情報処理システムの中のメーカー用情報処理装置における処理内容を示すフローチャートである。

【図4】本発明の一実施形態による電子クーポン装置を用いる情報処理システムの中の購入者用情報処理装置及び購入者の所有するICカードにおける処理内容を示すフローチャートである。

【図5】本発明の一実施形態による電子クーポン装置を用いる情報処理システムの中の小売店用情報処理装置及び購入者が所持したICカードにおける処理内容を示すフローチャートである。

【図6】本発明の一実施形態による電子クーポン装置によって生成される割引クーポンのデータ構成の説明図である。

【符号の説明】

100, 100A…ICカード

110…ICカードチップ

16

*112…外部接続インタフェース

114…マイクロプロセッサ

116…記憶部

116A…プログラムロード格納エリア

116B…暗号処理プログラム格納エリア

116C…クーポン生成プログラム格納エリア

116D…クーポン署名用秘密鍵格納エリア

116E…復号用暗号鍵格納エリア

116F…購入履歴格納エリア

116G…ワークエリア

200…インターネット

210…メーカー用情報処理装置

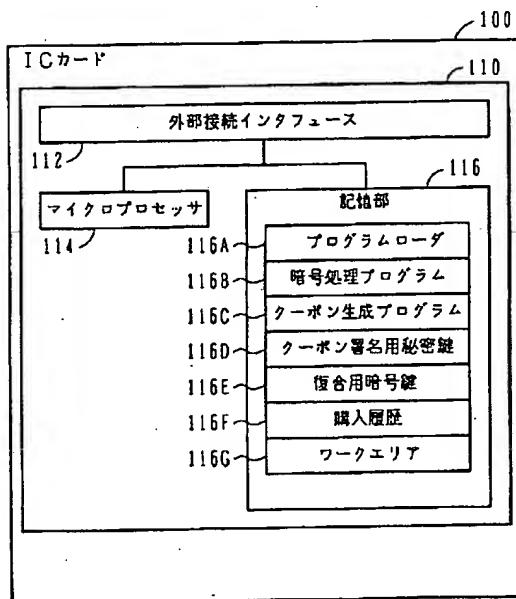
220…購入者用情報処理装置

222, 232…ICカードリーダライタ

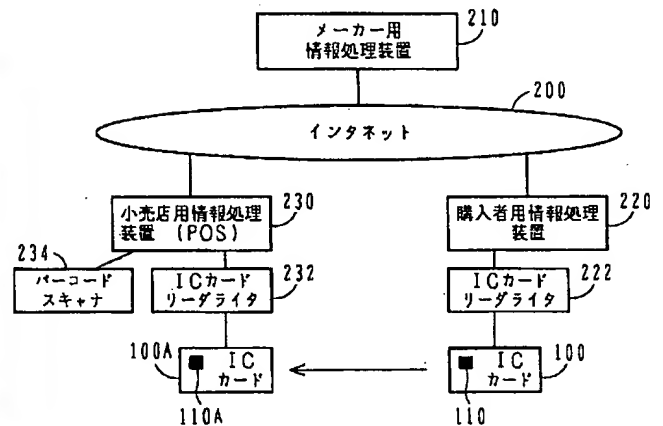
230…小売店用情報処理装置

234…バーコードスキャナ

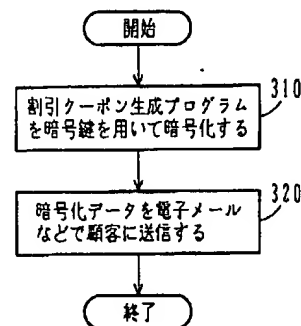
【図1】



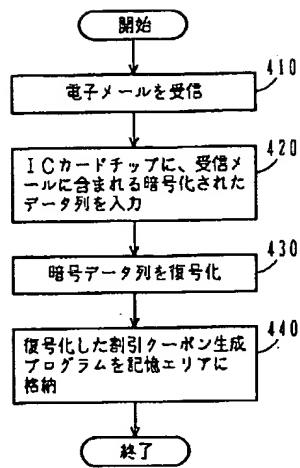
【図2】



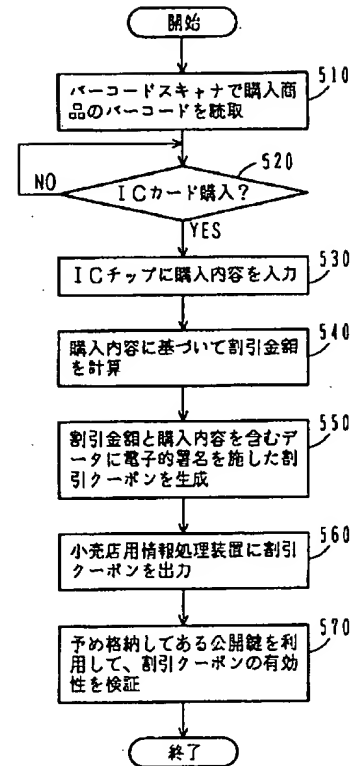
【図3】



【図4】



【図5】



【図6】

